

Myths and Facts about EPC-Enabled RFID and Its Use in Identification Documents

EPCglobal US facilitates the responsible deployment of Electronic Product Code™ (EPC) enabled Radio Frequency Identification (RFID) technology, while helping to expand its use to benefit the public, businesses, and government. The primary use of EPC-enabled RFID is in business, helping trading partners to track products and other items as they make their way from factory or field to the consumer.

Recently some myths have been spread about EPC-enabled RFID and a secondary application, in personal identification documents like Passport Cards and enhanced driver's licenses. The following document faces these myths head on so you can make your own informed decisions about a technology with the ability to protect lives, reduce costs for businesses and prices for consumers, reduce energy use, and other transformative benefits.

Myths	Facts
<p>Myth: EPC-enabled RFID identity cards, such as U.S. Passport Cards and Enhanced Drivers Licenses, carry personal information, which can be easily read/skimmed by someone with an RFID receiver/reader.</p>	<p>RFID chips contain no personal information, just a string of numbers. This number string is useful only when indexed through one or more highly secure databases. Without such access, no personal information can be obtained.</p> <p>Note: EPC-enabled RFID chips have limited capacity. They contain only a unique set of numbers that identify the product or thing in which the chip is embedded. Just like the common barcode, it is only when those numbers are matched through one or more secure databases that a connection is made.</p> <p>Further, the tag in an EPC chip has no power source and can only transmit its unique number up to 20 feet from a reader that activates the tag (the greater distance would be only under ideal conditions). Even if someone did illegally "skim" a number, or use an illegal reader, any numbers they obtain are essentially meaningless because they cannot access secure databases.</p>
<p>Myth: Putting an EPC reader and credit-card RFID reader at a checkout line, or other "chokepoint", can allow a hacker to skim both of them and associate them to build a data profile of a person and track that person no matter where they go.</p>	<p>This scenario, in practical terms, is essentially impossible. RFID-enabled credit cards (a small percentage of credits cards in circulation) must be within 2-3 inches of a reader to be read. The card holder would have to pass through a portal that can read two separate radio frequencies AND for some reason walk in such a way to put their credit card within extremely close proximity of that reader.</p> <p>Even if this could somehow be done, the result would be two random numbers, neither of which reveals personal information without access to highly secure databases.</p>
<p>Myth: Hackers can buy parts to scan RFID tags from Passport Cards and make a fake Passport Card ("clone the tag").</p>	<p>The tag contains only a unique number and no personal information. A copied tag has no value for a border crossing because the crossing process requires a visual match between the driver and photo retrieved from a secure database record.</p>
<p>Myth: Hackers can build readers that can read chips from miles away.</p>	<p>Not true, under the most favorable conditions, without interference, the maximum distance the EPC standard tag can be read is 6 meters or about 20 feet.</p>
<p>Myth: With available technology, a hacker can "rewrite" or change the EPC/unique ID on a tag carried by someone else, effectively changing their identity.</p>	<p>The EPC number can be left open or permanently locked for different applications. EPCglobal US strongly advises document issuers using the EPC to lock it after writing the EPC to the tag. In addition, write-access to RFID tags can be password-protected to further deter tag alteration.</p>

